New Frontiers in Risk-Based Design for Exploration

Dr. Francesca Barrientos

Design for Systems Safety and Reliability
francesca.a.barrientos@nasa.gov

Computational Sciences Division

NASA Ames Research Center

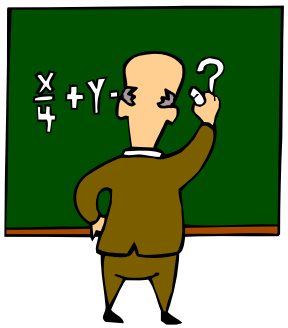
Risk-Based Design

Risk-Based design uses formal methods to:

a) understand and characterize risk drivers as the design develops, and

b) incorporate risk information into principles methodologies or tools that enable engineers to make design decisions that reduce risk while meeting the overall goals of the system.

Risk-Based Design Research Activities

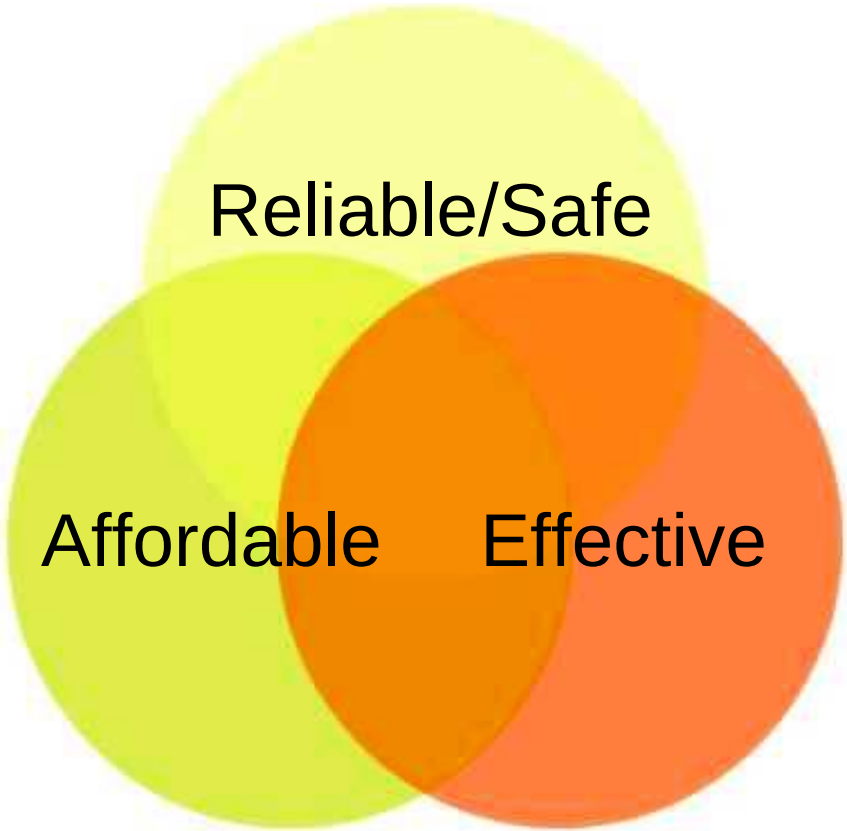


Research formal design theories and methods for rationally and explicitly accounting for sources of risk in design choices

Develop tools and methodologies to integrate risk-based design methods into the design process

Work with engineers to understand how risk is managed during design

Sustainable Exploration Challenges



Vision for Exploration demands dramatic increases in system reliability, affordability and effectiveness

Risk-based design methods impact exploration challenges at design time

Outline

- Risk-based design research
  - Research group at ARC
  - Focus on early stage design
- Example project
  - Function Failure Design Tool
- Other projects and future directions

Here to learn from SMA community

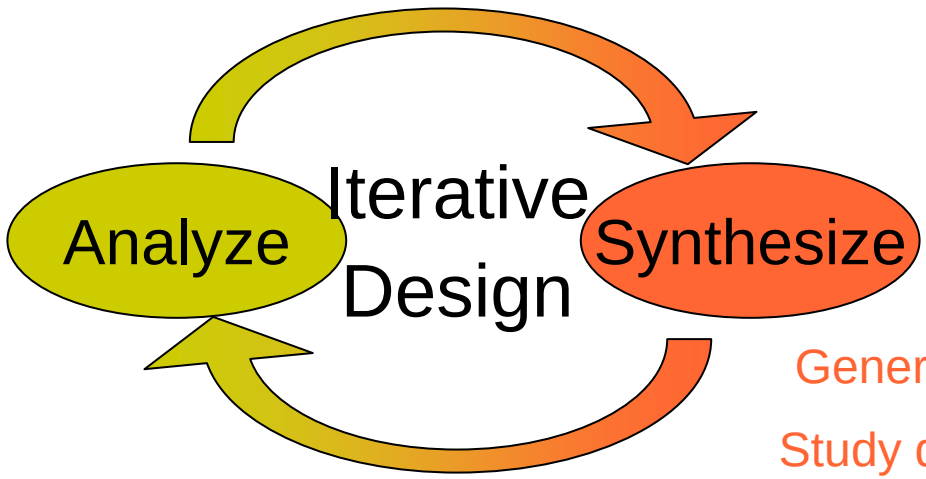
- What should we know about?
- How does design fit into the risk management process?
- How can risk and failure assessment be applied to design?
- What tools are used and how?

Risk Assessment and Decision-making in Design Tasks

Open questions:

How to perform risk analysis during different design stages

How to use risk information during design tasks



Assess risks

Assess failure modes

Generate concepts

Study design trades

Select architectures

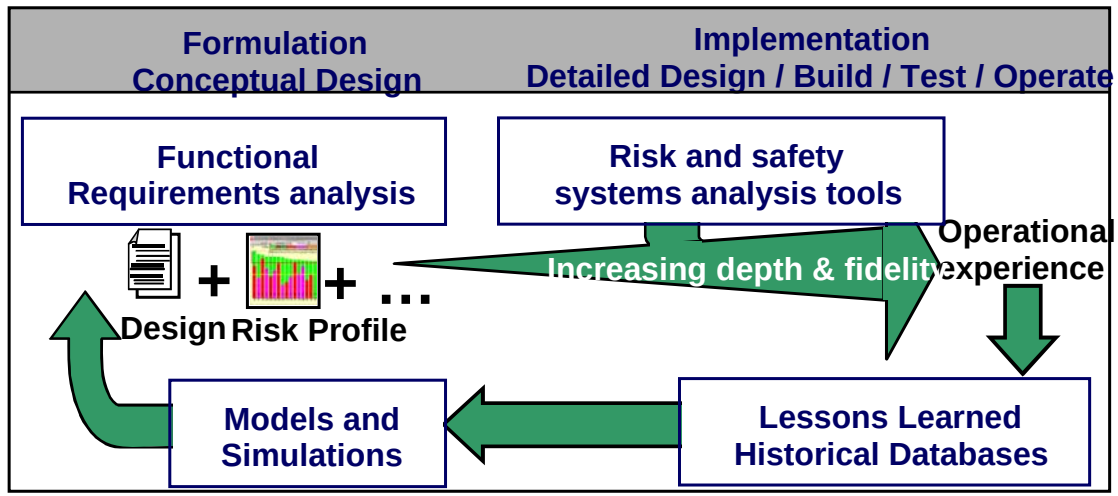
Optimize parameters

Focus: Risk During Conceptual Design

- Early stage design characteristics
  - Functional requirements partially identified
  - Few hardened solutions or physical specifications
- Assertion: More effective to mitigate risks and and design against failures at early stage of design than at later stages
- Opportunities
  - Best time to catch potential failures and anomalies
  - Redesign costs are lowest during early design
  - Engineers can explore larger design space because decisions have not yet been made

Managing Risk During Design Lifecycle at NASA

- "Risk-based design" usually means quantitative methods
  - Usually refers to PRA
  - Other parameterized probabilistic, quantitative models
- Reliability methods applied to design
  - Eg. FMEA/FMECA
  - FTA
  - ETA
- Historical Databases
  - LLIS
  - PRACA
  - PF/R



Early Stage Design Challenges

- Risk assessment and failure modes analysis methods
  - Developed for detailed design stage when re-design is costly
  - PRA not practical/feasible at the early design stages
  - Existing failure identification tools (FMEA, FTA) are tedious, experience-based, and system-specific
  - Hazard analysis tools system specific
- Lessons-learned databases
  - Information is system specific
  - Information goes in and stays there
  - No systematic way to search for information that is relevant to new designs
  - Lack methods to generalize historical knowledge (PRACA, P/FR, LLIS) for re-use in subsequent designs

More Early Design Stage Challenges

- Vast design space to explore and consider
- Preponderance of unknowns and uncertainties- (decisions not yet made; no physical forms chosen)
- Risk is not formally used as a tradeoff factor
- No systematic methods to optimize risk in design trades

Basic Risk-Based Design Research

- Formal methods
  - Quantify uncertainty in design decisions using mathematical models
  - Use formal methods to rationalize decision-making in design

Research areas:

Reliability
Risk Analysis
Optimization
Decision-based design
Design Under Uncertainty
Probabilistic design
Robust Design
Visualization

Study Conceptual Design Environments

- Study work practice in concurrent engineering environments:
  - PDC at JPL
  - IMDC at GSFC
- Develop tools/methods
- Test and validate in similar environments

Function Failure Design Tool

Injects risk mitigation into early design

- ✓ Given subsystem functionality, how might it fail?
- ✓ Can we add new functionality to safeguard or change the functionality to avoid the failure?
- ✓ Can we learn from different systems with similar functionality and failure modes?

Knowledge base

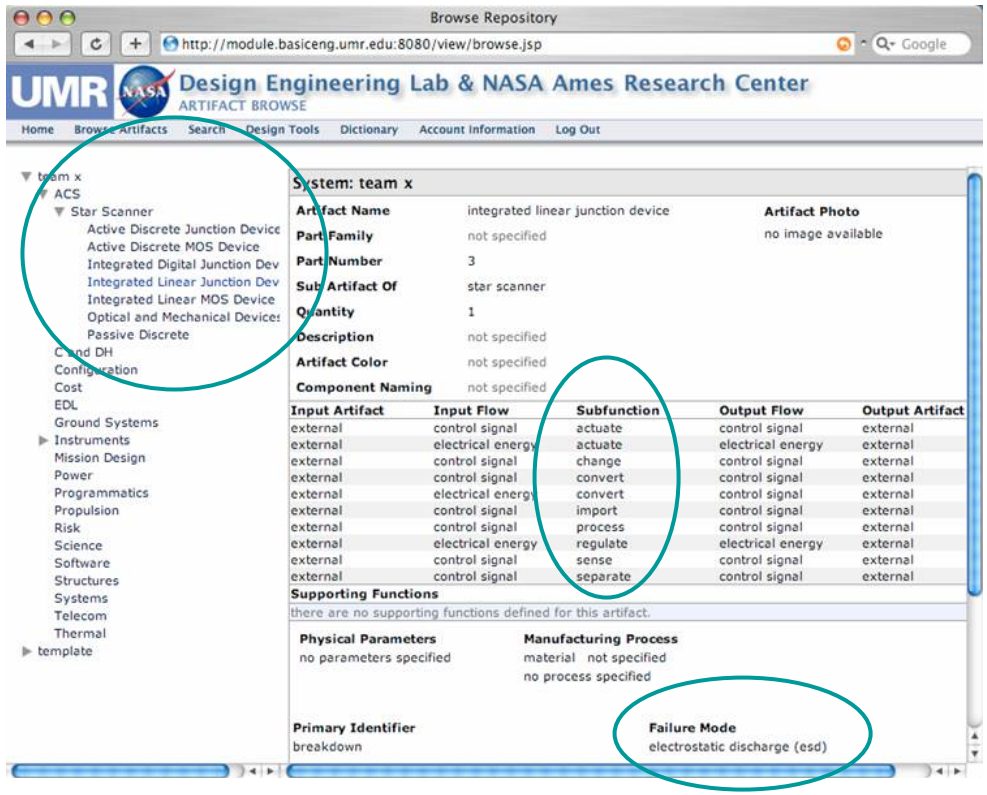
- Form: systems, subassemblies and components from existing JPL mission studies
- Function: models of existing subsystems
- Failure modes: extracted from historical documents

Multiple views into knowledge

- What failures or risks are associated with this subsystem?
- What failures are associated with this function?

Functional models

- Form independent: generic and reusable
- Suits conceptual design phase



Design tool for generating potential failure failure and risk lists

Function Failure Design Method

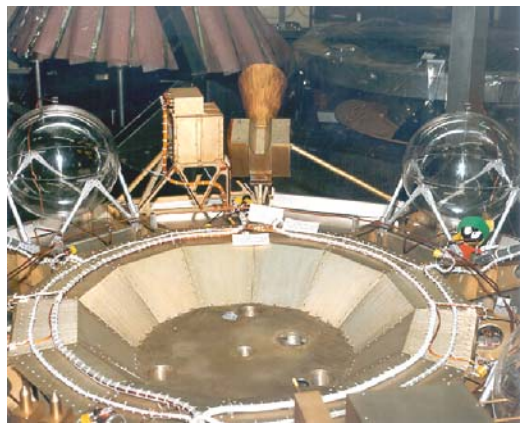
Formal elements

- Functional taxonomy spans all electro-mechanical functions
- Developed failure-mode taxonomy
- Repository of existing designs

Implementation approach

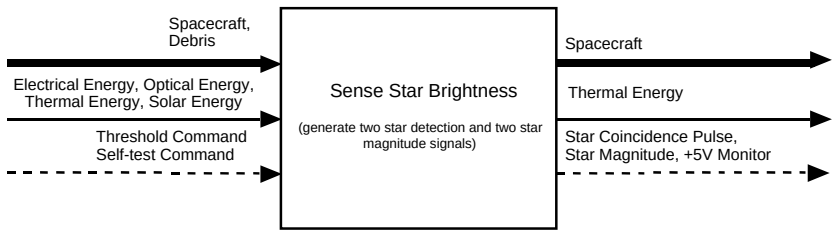
- Bottom-up: build functional models of existing subsystems (generic and reusable)
- Generate list of failures from these subsystems (failure reports, FMEAs)
- Map function to failures to create function-failure knowledge bases

Developed by Dr. Irem Tumer, ARC
with Prof. Robert Stone, UMR



Ex: Probe Cruise Stage: Star Scanner Assembly

Black box functional model is the highest level description of system:



Related Projects at ARC
Design for Systems Safety and Reliability

- Group: Dr. Irem Tumer (lead), Dr. Francesca Barrientos, Dr. Eric Barszcz
- Collaborators on current projects:
  - Errors in design reviews (with Kos Ishii/ Stanford)
  - Co-design of ISHM with functional design (NASA and Boeing Rocketdyne)
  - Decision management for human-agent design teams (with D. Ullman/RDI)
  - Modeling uncertainty in design (with C. Paredis/GaTech)
  - Sensor selection for ISHM design (A. Agogino/UC Berkeley)
  - Design Variability analysis for fault detection (with Dan McAdams/UMR)

Future projects pending funding:

- Activity awareness in distributed collaborative design environments (with C.Hayes/UMN and M. Dorneich/Honeywell)
- Design environment for failure recovery for robotic servicers (with M. McCarthy/UCI)
- Risk assessment with Probability Bound Analysis (with C. Paredis and Lockheed)
- Trade studies and decision making under uncertainty (with D. Ullman/RDI)
- Model based design for ISHM (with Vanderbilt and Boeing Rocketdyne)

Summary

- Introduction to Risk-based design research at ARC
- Focus on early stage (conceptual, functional) design stage
- Real applications and engineers at NASA shape the implementation of new tools
  - Example: FFDT
- NASA is collaborating with many of the leaders in design theory and methods research

Questions? Discussion! Ideas…

Further information:

Design for Systems Safety and Reliability Group
Computational Sciences Division
NASA Ames Research Center

Dr. Irem Tumer
Group Lead
itumer@mail.arc.nasa.gov

Dr. Francesca Barrientos
francesca.a.barrientos@nasa.gov